UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/536,650	05/26/2005	Stephen Brian Morris	P/63699	2473

156 7590 03/20/2008

KIRSCHSTEIN, OTTINGER, ISRAEL
& SCHIFFMILLER, P.C.
489 FIFTH AVENUE
NEW YORK, NY 10017

EXAMINER	
TURNER, ASHLEY D	

ART UNIT	PAPER NUMBER
2154	

MAIL DATE	DELIVERY MODE
03/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/536,650	MORRIS, STEPHEN BRIAN	
	Examiner	Art Unit	
	ASHLEY D. TURNER	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *22-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *22-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/26/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 22 - 42 are rejected under U.S.C.101 because the claimed invention is directed to non-statutory subject matter.

Independent claim 22 is drawn towards "A telecommunications network, a route object (RO) computer program product, comprising: means for creating the RO which presents a user with editable fields relating to more that one type of RO, and allows the user to specify contents of at least one of the fields to create any one of the types of the RO. In order for a claim to be statutory, it must result in useful, concrete, tangible results. In this instance case, computer program product is not implemented on storage medium. This implies it could be software per se, which is not one of the four statutory categories. As such, the subject matter of the claim is not patent eligible.

Claims 23-39 fail to solve the deficiencies of claim 22 and thus are rejected for the same.

Independent claims 40, 41 and 42 are rejected for the same reasoning as claim 22 which is described above.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 22-42 are rejected under 35 U.S.C102 (b) as being anticipated by Myerson et al hereinafter Bays (U.S. 2003/0204619 A1).

Regarding Claim 22

Referring to claim 22 Bays discloses In a telecommunications network, a route object (RO) computer program product, comprising: means for creating the RO which presents a user with editable fields relating to more than one type of the RO (Pg. 13 lines 5-9 The data collector 90 will then send a second packet with the TTL set to two to determine the next intermediate system in the path. This process is repeated until a complete intermediate system hop-by-hop path is created for the destination network. This list is the set of all ingress interfaces the path passes through on each intermediate system in route to the destination network.)

(Paragraph [0041] The user must supply a nominal amount of information to have routing control device 20 configure a new peer (e.g., an inter-domain peer or internal peer) or modify an existing one. Minimally, the user provides routing control device 20 with the name of the routing system 30 being configured and the IP address of the peer (e.g., inter-domain peer 60 or 62 or internal peer 34) (FIG. 6, step 502). Optionally, the user can supply routing control device 20 with additional policy requirements for this peer such as peer-specific filtering or transit parameters.), and allows the user to specify contents of least one of the fields to create any one of the types of the RO (Paragraph [0059] Once a destination peer is selected, the network is routed over that peer by injecting a BGP route update into the routing system 30 with the next hop field set to the destination peer's address, using techniques as described in section 1.2.2).

Regarding Claim 23

Referring to claim 23 Bays discloses all the limitations of claim 23 which is described above. Bays also discloses in which the RO presents the at least one editable field relating to a type of route defined by the RO (Paragraph [0059] Once a destination peer is selected, the network is routed over that peer by injecting a BGP route update into the routing system 30 with the next hop field set to the destination peer's address, using techniques as described in section 1.2.2).

Regarding Claim 24

Referring to claim 24 Bays discloses all the limitations of claim 24 which is described above. Bays also discloses in which the RO presents at least one editable field relating to at least one network element (NE) of a route through the telecommunications network defined by the RO.(Paragraph [0059] The peer set is then reordered so that the chosen peer becomes the last available element in the set and the next destination peer becomes the first available element in the set (step 826). This process is repeated for each destination network in the list up to the user-defined limit (see steps 820 and 832).

Regarding Claim 25

Referring to claim 25 Bays discloses all the limitations of claim 25 which is described above. Bays also discloses in which each type of RO comprises at least one hop, and the RO computer program product presents at least one editable field relating to the at least one hop of the RO. (Paragraph [0059] Once a destination peer is selected, the network is routed over that peer by injecting a BGP route update into the routing system 30 with the next hop field set to the destination peer's address, using techniques as described in section 1.2.2).

Regarding Claim 26

Referring to claim 26 Bays discloses all the limitations of claim 26 which is described above. Bays also discloses in which, when the user specifies the contents of the at least

one editable field, at least one of the specified field and the specified contents is used by the RO computer program product to determine which subsequent editable field is presented to the user. (Pg. 4 paragraph [0042] This is accomplished by retrieving the current peering configuration from the routing system 30 (step 506), translating it into a system rule set, and comparing it to the version stored in routing control device database 24 (see steps 504 and 508). If the system rule sets do not match (step 508), a warning is issued (step 510) and by default the action is aborted. However, the user may specify that if the retrieved system rule set does not match the stored system rule set, routing control device 20 should overwrite the existing configuration using the new stored system rule set (step 512). Once the system rule sets have been compared, the user supplies data explaining the desired policy outcome by responding to questions from a predefined template (step 514). This data is combined with the previously stored system rule set to generate an inclusive view of the desired routing policy for that peer (step 516). This inclusive system rule set is interpreted against the primary configuration policy and formatted to generate the new peer configuration. The completed rule set is verified for consistency with network wide policy and translated to the proper configuration nomenclature for the routing system (step 518). Unless otherwise instructed by the user (see step 520), routing control device 20 will use the previously stored default access method for the routing system to apply the new configuration (step 522). The user has the option, however, of overriding this step and choosing to apply the configuration generated by the routing control device 20 manually to the routing system. Finally, the old system rule set is replaced with the new one in routing control device database 24 (step 524).

Regarding Claim 27

Referring to claim 27 Bays discloses all the limitations of claim 27 which is described above. Bays also discloses in which, when the user specifies the contents of the at least one editable field, at least one of the specified field and the specified contents is used by the RO computer program product to determine at least one default setting of at least one subsequent editable field presented to the user. (Paragraph [0033] Routing control device 20 includes a predefined or default routing policy configuration, called the default device configuration policy. In one embodiment, the default routing policy configuration is stored in routing control device database 24. This set of routing policies defines a default configuration rule set that determines how inter-domain routing should be configured based on current industry best practices. All actions routing control device 20 makes are directly or indirectly based on this default configuration rule set. The user can update the default device configuration policy periodically by querying a central server (e.g., such as a server located at routing control center 25) and downloading the latest default device configuration policy, if desired. The user can further modify the default device configuration policy to apply customized network wide configuration parameters by supplying the requested policy as a local configuration policy that is input to routing control device 20 using a graphical interface, a configuration file, or a command line interface. This local configuration policy is checked for errors based on the specifications of

the default device configuration policy. The local configuration policy is then saved in routing control device database 24, over-writing any previously saved local configuration policies. Each time routing control device 20 is powered on it reads the local configuration policy from routing control device database 24 and if it exists, combines it with the default configuration policy. This combined policy becomes the primary configuration policy for routing control device 20. In one embodiment, a user may specify a local configuration policy for each routing system 30; routing control device 20 therefore generates a primary configuration policy for each routing system 30.)

Regarding Claim 28

Referring to claim 28 Bays discloses all the limitations of claim 28 which is described above. Bays also discloses and comprising means for modifying at least one RO. (Paragraph [0041] The user must supply a nominal amount of information to have routing control device 20 configure a new peer (e.g., an inter-domain peer or internal peer) or modify an existing one. Minimally, the user provides routing control device 20 with the name of the routing system 30 being configured and the IP address of the peer (e.g., inter-domain peer 60 or 62 or internal peer 34) (FIG. 6, step 502).

Regarding Claim 29

Referring to claim 29 Bays discloses all the limitations of claim 29 which is described above. Bays also discloses comprising means for copying at least one RO. (Paragraph

[0073] An Internet Control Message Protocol (ICMP) TTL expired error response is sent back to the source of the packet with a copy of the expired packet's IP header plus the first 8 bytes of the payload. See F. Baker, Cisco Systems, Inc., Network Working Group, "Requirements for IP Version 4 Routers," RFC 1812, June 1995. For example, a packet sent with a TTL value of three would be able to traverse three intermediate systems before expiring or "timing out." Per RFC 1812, the third intermediate system would discard the packet and send an ICMP response back to the sender).

Regarding Claim 30

Referring to claim 30 Bays discloses all the limitations of claim 30 which is described above. Bays also discloses and comprising means for storing at least one RO in a storage facility.(Paragraph [0115] For example, routing control device 20 can be deployed in a stand-alone configuration or as part of a centrally managed service. In addition, routing control device 20 can operate in connection with a centralized routing control database 42 storing routing path information gathered by a plurality of data collectors 90 connected to an autonomous system (see FIG. 2). Moreover, the functionality described herein can be incorporated into a centralized routing policy management service requiring no equipment at the customer's site.)

Regarding Claim 31

Referring to claim 31 Bays discloses all the limitations of claim 31 which is described above. Bays also discloses comprising means for deleting at least one RO. (Paragraph [0038] The user may request the system rule set for the deleted routing system to continue to be stored in routing control database 24 for future use after being marked as inactive by routing control device 20 (see steps 414 and 418). If left in routing control device database 24, the system rule set will not affect any routing control device 20 decisions as long as it is marked inactive. If the system rule set is not marked inactive, routing control device 20 removes it from the routing control device database 24 (step 416)).

Regarding Claim 32

Referring to claim 32 Bays discloses all the limitations of claim 32 which is described above. Bays also discloses comprising means for discovering at least one RO. (Pg. 4 [0042] Optionally, the user can supply routing control device 20 with additional policy requirements for this peer such as peer-specific filtering or transit parameters. Each time a new peering configuration-that is, the portion of the system rule set specific to the peer-is generated, the peering configuration state on the routing system 30 is compared with the last known good peering configuration saved in the routing control device database 24, if one exists, to ensure consistency and to detect any non-routing-control-device-20-introduced changes. This is accomplished by retrieving the current peering configuration from the routing system 30 (step 506), translating it into a system rule set, and comparing it to the version stored in routing control device database 24 (see steps 504 and 508). If the system rule sets do not match (step 508), a

warning is issued (step 510) and by default the action is aborted. However, the user may specify that if the retrieved system rule set does not match the stored system rule set, routing control device 20 should overwrite the existing configuration using the new stored system rule set (step 512). Once the system rule sets have been compared, the user supplies data explaining the desired policy outcome by responding to questions from a predefined template (step 514).)

Regarding Claim 33

Referring to claim 33 Bays discloses all the limitations of claim 33 which is described above. Bays also disclose comprising means for discovering changes in the telecommunications network. (Pg. 12 paragraph [0122] Routing control device 20 resides at the customer site, but is run centrally at the Routing Control Center (ARCC@) 25. Through a graphical user interface presented by a web server at the RCC 25, the customer, using an Internet browser, directs the RCC 25 to conduct changes to the appliance 20 on their behalf. The RCC 25 connects directly to the customer premise appliance 20 in a secure manner to modify the modules as required. The customer is able to monitor the system through a Web interface presented by the RCC 25 and view reports on network statistics.)

Regarding Claim 34

Referring to claim 34 Bays discloses all the limitations of claim 34 which is described

above. Bays also discloses comprising means for interfacing with the user (Pg.2 paragraph [0031] The user may add routing systems 30 to routing control device 20 by supplying the IP address or fully qualified domain name of a primary interface and access authority information for the routing system (FIG. 3, step 204). Optionally, routing control device 20 may import a set of routing systems from an external source or via a system discovery protocol (FIG. 3, step 206). A primary interface is one that has a known IP address or a fully qualified domain name assigned for the duration of the life of the routing system. Access authority information usually consists of a user name, password combination but may contain other necessary information for a specific authentication protocol and should be supplied for each type of access method supported by routing control device 20 (see step 202). Access methods include Simple Network Management Protocol (SNMP) queries, interactive sessions to terminal interfaces, and other proprietary access protocols.

Regarding Claim 35

Referring to claim 35 Bays discloses all the limitations of claim 35 which is described above. Bays also disclose in which the means for interfacing presents a same interface to the user regardless of the type of the RO to be created. (Pg. 3 paragraph [0036] In particular and in one embodiment, once a routing system has been added to routing control device 20 initially, the routing system 30 must be configured. Subsequent changes in the primary device configuration policy may also require the routing system 30 to be reconfigured. To do this, the user specifies the routing system(s) 30 to be configured (FIG. 4, step 302). Query

methods and access authority information are retrieved for the corresponding IP addresses or fully qualified domain names from routing control device database 24 (step 304). Routing control device 20 then queries the routing systems 30 to assemble a current routing system configuration for each routing system 30 using the appropriate query method (step 306). The retrieved routing system configuration is interpreted to define the current BGP peering setup as a rule set per routing system called a system rule set (step 308). This system rule set includes the entire data set of configuration information for the peers such as IP addresses, autonomous systems, filters, descriptions, and peering options. If the retrieved system rule set is in conflict with the primary device configuration policy of routing control device 20, routing control device 20 logs an error, fixes the system rule set (step 312), and applies the updated system rule set to the routing system 30 (step 314). The finalized system rule set is stored in the routing control database 24 for later retrieval (step 316). Parameters in the system rule set may be translated into user-friendly names using a proprietary database of information. For example routing control device 20 may map autonomous system numbers to network names.

Regarding Claim 36

Referring to claim 36 Bays discloses all the limitations of claim 36 which is described above. Bays also discloses in which the means for interfacing comprises a graphical user interface (GUI) which presents at least one window to the user, to allow the user to create the RO. (Pg.3 paragraph [0033] The user can update the default device configuration policy periodically by querying a central server (e.g., such as a server located at routing control center 25) and downloading the latest default device configuration policy, if desired. The user

can further modify the default device configuration policy to apply customized network wide configuration parameters by supplying the requested policy as a local configuration policy that is input to routing control device 20 using a graphical interface, a configuration file, or a command line interface.)

Regarding Claim 37

Referring to claim 37 Bays discloses all the limitations of claim 37 which is described above. Bays also discloses in which the GUI presents a network element (NE) listing window to the user which comprises a NE context menu having a create RO menu item which brings up a window comprising a RO creation dialog box, which comprises at least one editable field relating to at least one type of RO, and the user specifies the contents of at least one of the fields to create any one of the types of RO. (Pg. 12 [0118] As an appliance, routing control device 20 is a standalone box that runs on a kernel based operating system. The kernel runs multiple modules, which handle the individual tasks of routing control device 20. For example, the appliance may comprise a Linux-based server programmed to execute the required functionality, including an Apache web server providing an interface allowing for configuration and monitoring. Modules are proprietary code that implements the policy and engineering functions described above. Additionally, the kernel handles system functions such as packet generation and threading. Routing control device 20 includes one or more network interfaces for peering and traffic sampling purposes. An included BGP protocol daemon is responsible for peering and for route injection. A web server daemon provides a

graphical front end.)

Regarding Claim 38

Referring to claim 38 Bays discloses all the limitations of claim 38 which is described above. Bays also discloses in which the RO being created comprises at least one hop, and the at least one hop is added to the RO using a window comprising a hop creation dialog box, which comprises at least one editable field relating to at least one type of hop, and the user specifies the contents of at least one of the fields to create any one of the types of hop. (Pg. 5 paragraph [0059] An ordered set of inter-domain peers to be balanced is generated from the IP addresses supplied by the user (step 806). In one preferred form, the first element of the set is the active peer for the largest destination network. To most appropriately load share across the available inter-domain peers, the results from a load sharing algorithm are used to select the destination peer for each network (see steps 834, 836, 838 and 840). First, the destination network's current traffic load figures are subtracted from its present destination peer's total traffic load figures (step 824). The destination network is then compared to each destination peer in the set in turn until a suitable path is found or the entire set has been traversed (see steps 828, 834, 836,838 and 840). To find a suitable path, the first destination peer in the set is chosen (step 834) and the network is verified to be reachable through it (step 836). If so, the destination peer's current traffic load is verified to insure sufficient bandwidth is available to handle the additional burden of the destination network (step 840). If the bandwidth is available the destination peer is chosen as the best path (step 842). If neither of these expectations are met, the

next destination peer in the set is analyzed against the network using the same methods (step 838). The process is repeated for the destination network until an available peer can be found or the entire set has been traversed (see step 828). If no suitable destination peer is found, then the destination peer with network reachability and the greatest available bandwidth is chosen (step 830). Once a destination peer is selected, the network is routed over that peer by injecting a BGP route update into the routing system 30 with the next hop field set to the destination peer's address, using techniques as described in section 1.2.2. The peer set is then reordered so that the chosen peer becomes the last available element in the set and the next destination peer becomes the first available element in the set (step 826). This process is repeated for each destination network in the list up to the user-defined limit (see steps 820 and 832).

Regarding Claim 39

Referring to claim 39 Bays discloses all the limitations of claim 39 which is described above. Bays also discloses in which the RO being created comprises a group RO, and the GUI presents a network element (NE) listing window to the user which comprises a NE context menu having a create group RO menu item which brings up a window comprising a group RO creation dialog box, which comprises at least one editable field relating to at least one type of group RO, and the user specifies the contents of at least one of the fields to create any one of the types of group RO. (Pg. 5 paragraph [0059] An ordered set of inter-domain peers to be balanced is generated from the IP addresses supplied by the user (step 806). In one preferred form, the first element of the set is the active peer for the

largest destination network. To most appropriately load share across the available inter-domain peers, the results from a load sharing algorithm are used to select the destination peer for each network (see steps 834, 836, 838 and 840). First, the destination network's current traffic load figures are subtracted from its present destination peer's total traffic load figures (step 824). The destination network is then compared to each destination peer in the set in turn until a suitable path is found or the entire set has been traversed (see steps 828, 834, 836,838 and 840). To find a suitable path, the first destination peer in the set is chosen (step 834) and the network is verified to be reachable through it (step 836). If so, the destination peer's current traffic load is verified to insure sufficient bandwidth is available to handle the additional burden of the destination network (step 840). If the bandwidth is available the destination peer is chosen as the best path (step 842). If neither of these expectations are met, the next destination peer in the set is analyzed against the network using the same methods (step 838). The process is repeated for the destination network until an available peer can be found or the entire set has been traversed (see step 828). If no suitable destination peer is found, then the destination peer with network reachability and the greatest available bandwidth is chosen (step 830). Once a destination peer is selected, the network is routed over that peer by injecting a BGP route update into the routing system 30 with the next hop field set to the destination peer's address, using techniques as described in section 1.2.2. The peer set is then reordered so that the chosen peer becomes the last available element in the set and the next destination peer becomes the first available element in the set (step 826). This process is repeated for each destination network in the list up to the user-defined limit (see steps 820 and 832).

Regarding Claim 40

Referring to claim 40 Bays discloses A method of creating a route object (RO), comprising the steps of: running a RO computer program product which creates the RO which presents editable fields relating to more than one type of the RO; and specifying contents of at least one of the fields to create any one of the types of the RO. (Pg. 4 paragraph [0042] This is accomplished by retrieving the current peering configuration from the routing system 30 (step 506), translating it into a system rule set, and comparing it to the version stored in routing control device database 24 (see steps 504 and 508). If the system rule sets do not match (step 508), a warning is issued (step 510) and by default the action is aborted. However, the user may specify that if the retrieved system rule set does not match the stored system rule set, routing control device 20 should overwrite the existing configuration using the new stored system rule set (step 512). Once the system rule sets have been compared, the user supplies data explaining the desired policy outcome by responding to questions from a predefined template (step 514). This data is combined with the previously stored system rule set to generate an inclusive view of the desired routing policy for that peer (step 516). This inclusive system rule set is interpreted against the primary configuration policy and formatted to generate the new peer configuration. The completed rule set is verified for consistency with network wide policy and translated to the proper configuration nomenclature for the routing system (step 518). Unless otherwise instructed by the user (see step 520), routing control device 20 will use the previously stored default access method for the routing system to apply the new configuration

(step 522). The user has the option, however, of overriding this step and choosing to apply the configuration generated by the routing control device 20 manually to the routing system. Finally, the old system rule set is replaced with the new one in routing control device database 24 (step 524).

Regarding Claim 41

Referring to claim 41 Bays discloses A network management system (NMS), comprising: a route object (RO) computer program product including means for creating the RO which presents a user with editable fields relating to more than one type of the RO, and allows the user to specify contents of at least one of the fields to create any one of the types of the RO. (Pg. 4 paragraph [0042] This is accomplished by retrieving the current peering configuration from the routing system 30 (step 506), translating it into a system rule set, and comparing it to the version stored in routing control device database 24 (see steps 504 and 508). If the system rule sets do not match (step 508), a warning is issued (step 510) and by default the action is aborted. However, the user may specify that if the retrieved system rule set does not match the stored system rule set, routing control device 20 should overwrite the existing configuration using the new stored system rule set (step 512). Once the system rule sets have been compared, the user supplies data explaining the desired policy outcome by responding to questions from a predefined template (step 514). This data is combined with the previously stored system rule set to generate an inclusive view of the desired routing policy for that peer (step 516). This inclusive system rule set is interpreted against the primary configuration policy

and formatted to generate the new peer configuration. The completed rule set is verified for consistency with network wide policy and translated to the proper configuration nomenclature for the routing system (step 518). Unless otherwise instructed by the user (see step 520), routing control device 20 will use the previously stored default access method for the routing system to apply the new configuration (step 522). The user has the option, however, of overriding this step and choosing to apply the configuration generated by the routing control device 20 manually to the routing system. Finally, the old system rule set is replaced with the new one in routing control device database 24 (step 524).

Regarding Claim 42

Referring to claim 42 Bays discloses A method of setting up a connection of a telecommunications network, comprising the steps of: using a route object (RO) created using a RO computer program product operative for creating the RO, and presenting a user with editable fields relating to more than one type of the RO, and allowing the user to specify contents of at least one of the fields to create any one of the types of the RO. (Pg. 4 paragraph [0042] This is accomplished by retrieving the current peering configuration from the routing system 30 (step 506), translating it into a system rule set, and comparing it to the version stored in routing control device database 24 (see steps 504 and 508). If the system rule sets do not match (step 508), a warning is issued (step 510) and by default the action is aborted. However, the user may specify that if the retrieved system rule set does not match the stored system rule set, routing control device 20 should overwrite the existing configuration

using the new stored system rule set (step 512). Once the system rule sets have been compared, the user supplies data explaining the desired policy outcome by responding to questions from a predefined template (step 514). This data is combined with the previously stored system rule set to generate an inclusive view of the desired routing policy for that peer (step 516). This inclusive system rule set is interpreted against the primary configuration policy and formatted to generate the new peer configuration. The completed rule set is verified for consistency with network wide policy and translated to the proper configuration nomenclature for the routing system (step 518). Unless otherwise instructed by the user (see step 520), routing control device 20 will use the previously stored default access method for the routing system to apply the new configuration (step 522). The user has the option, however, of overriding this step and choosing to apply the configuration generated by the routing control device 20 manually to the routing system. Finally, the old system rule set is replaced with the new one in routing control device database 24 (step 524).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashley d. Turner whose telephone number is 571-270-1603. The examiner can normally be reached on Monday thru Friday 7:30a.m. - 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached at 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-270-2603.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Patent Examiner: Supervisory Patent Examiner

Ashley Turner Nathan Flynn

Date:_____ Date:_____

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2154